(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82167 A1

(51) International Patent Classification[7]: G06F 17/60, H04L 9/00

(21) International Application Number: PCT/SE01/00563

(22) International Filing Date: 19 March 2001 (19.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0001467-0 20 April 2000 (20.04.2000) SE

(71) Applicant and
(72) Inventor: PHILIPSON, Lars [SE/SE]; Bredgatan 7 B, S-222 21 Lund (SE).

(74) Agent: HANSSON THYRESSON PATENTBYRÅ AB; Box 73, S-201 20 Malmö (SE).

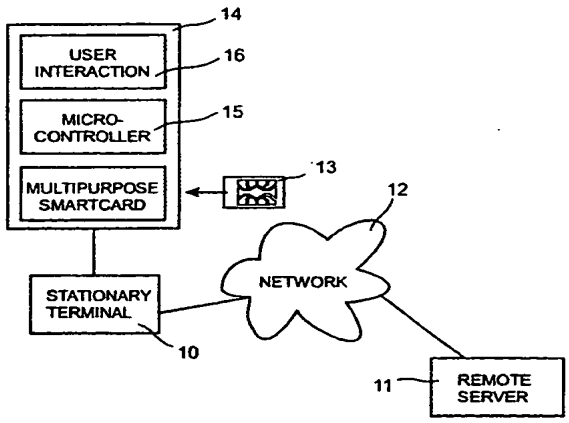
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: METHOD AND DEVICE FOR SECURE TRANSACTIONS




(57) Abstract: Method for secure digital data transactions, including the steps of: a) storing personal identification data, card identification data and a transaction program in a protected IC card, b) receiving personal identification data in said IC card, c) comparing said received personal identification data with said stored personal identification data and d) executing said transaction program when said personal identification data correspond to said stored personal identification data to establish contact between said IC card and a stationary terminal, e) mounting said IC card in a mobile unit, f) transferring said personal identification data to said IC card through said mobile unit, and g) further executing said transaction program to perform secure digital data transactions between said IC card and a stationary terminal through said mobile unit. The invention also comprises a device for secure digital transactions including an IC card (13) containing protected personal identification data, card identification data and a transaction program. The device includes a mobile terminal (14) comprising: a) receiving means (18) for receiving said IC card (13), b) input means (22) for entering personal identification data, c) communication means (23; 24) for performing secure digital data transactions between said IC card and a stationary terminal (10).

WO 01/82167 A1

# METHOD AND DEVICE FOR SECURE TRANSACTIONS

## BACKGROUND OF THE INVENTION

The field of this invention is authorization and authentication of a user during a transaction involving a stationary terminal or PC and possibly remote servers on a computer network. One of the means to provide security in such a situation is to use cryptography.

There are two main classes of encryption methods, symmetric and asymmetric. Symmetric encryption uses a secret key that is used both for encryption end decryption. This key has to be distributed beforehand to both parties and kept secret at all times. Asymmetric, or public key, encryption schemes uses a pair of keys where one can be public and the other must be secret. This makes key distribution much easier since the public key can be published and made available for instance over Internet.

## PRIOR ART

Independent of which encryption scheme that is used authentication requires a secret key. Smartcards (sometimes called IC cards) solve the problem of keeping the keys secret even if the card is lost. By encapsulating memory and processor into one tamper-resistant microchip and using PIN-codes and cryptography to protect access to the keys, a lost or stolen card cannot be used by any unauthorized person. When used the IC card is inserted into a stationary terminal having input means for entering the PIN code

However, the stationary terminal is a possible security leak. In a typical setting the user carries a set of smartcards and for every transaction inserts one of them in a smartcard reader. The reader could be connected e.g. to a point-of-sales terminal, an ATM machine, or to a personal computer. In order to unlock the card the user provides a PIN-code or a biometric sample (e.g. a fingerprint). The device to do this is part of the card reader or terminal equipment. It is technically possible to manipulate such equipment to break the security. For instance, the PIN-code or biometric sample could be recorded and used later.

The system disclosed in US5917913 solves this problem by providing the user with a portable electronic authorization device. All communication with the stationary terminal is encrypted and the user has full control of the reader, keyboard etc. This provides necessary conditions to prevent unauthorized access to information during a transaction. However, in a system according to US5917913 there is a problem of keeping the keys secret if the device is lost or stolen.

In summary, the following two security problems are associated with the use of cryptographic keys for authorization and authentication of a user during an electronic transaction.

- Keep the key secret even when the physical storage device is lost or stolen and
- prevent unauthorized manipulation of the equipment in order to get access to secret information during a transaction.

## SUMMARY OF THE INVENTION

An object of the present invention is to overcome both of the above mentioned problems.

The invention comprises a mobile terminal with a single built-in smartcard optionally capable of replacing a number of separate smartcards. The terminal contains means for user interaction and for communication with another terminal, that may be stationary or mobile (in the following called the stationary terminal).

Communication between the mobile and the stationary terminals can be based on wires or may be wireless, using IR, inductive couplings, radio, or any combination of those. The stationary terminal may be standalone, or connected to a network. In the latter case also one or several network servers could be involved in the transaction. Then the mobile terminal could act as an integral part of a distributed information system.

The smartcard is used primarily to store such data that must be protected if the device/card is lost or stolen. In a minimal configuration the following data is sufficient.

- Card identification (possibly implying also the identity of the user, an account number etc.)
- Secret cryptographic key (symmetric or asymmetric encryption)
- PIN-code or biometric reference

Access to the card is possible only by providing a PIN-code or biometric sample matching the stored reference. All communication between the mobile and stationary terminals is encrypted using the secret key or a separate session key exchanged by using the first key.

The terminal contains means for communication with the smartcard, with the stationary terminal and with the user. All of this can be built by using standard technology and the design of the terminal does not have to be kept secret. However, it must be provided by a trusted party in order not to have built-in security leaks.

Commercial documents, such as bank statements and receipts, are often produced as part of a transaction. The user may also want to keep other kinds of records, such as a time-stamped log. Using current technology most of this is either provided locally on paper or recorded electronically by the remote party. Both alternatives are inconvenient for the user. Ideally all documents related to a transaction should be stored in electronic form and easily be available to him in the future. Even when a smartcard is used, it has too limited storage space for this.

In one embodiment of the present invention this is accomplished by including a storage facility in the terminal where all relevant information can be recorded during the transaction. When convenient for the user the information can later be downloaded to a stationary computer or network for further processing and long time storage. All or part of the information can be protected by encryption using a key stored on the smartcard. Even if the terminal is lost together with the smartcard this information is protected. Optionally, documents can be protected by electronic signatures.

Integrating the smartcard into the mobile terminal causes potential problems for the user if he has several cards. Even for a single transaction it

may be relevant to use more than one card (e.g. a credit card and a bonus card). In one embodiment of the present invention this is accomplished by storing many virtual cards on one physical one, a multipurpose smartcard.

A multipurpose smartcard contains one ID part, common to all applications of the card, with

- Individual identification of the card
- At least one certificate of a cryptographic public key
- The corresponding private key(s)
- At least one PIN-code or biometric reference

Optionally the ID part also may contain information such as

- Name, photograph and other information about the card holder
- Expiration date and other restrictions that may apply to the card
- Information about the issuer of the card and its security references

This part of the card is written once and then protected so that it cannot be changed during the lifetime of the card.

The other main part of the protected memory of the smartcard is used for storing information specific to each individual application. Each entry in this area could optionally contain its own encryption key(s) or access code(s) in order to secure data and communication in addition to what is provided by the key(s) in the ID part. Such an entry constitutes a virtual card.

Virtual cards may be added and deleted after the physical card has been issued and distributed. The procedure of adding and deleting virtual cards can preferably be performed with the physical card residing in the terminal. Downloading of data corresponding to a virtual card can be protected by cryptographic protocols using the key(s) on the physical card. In this way a new virtual card can be added using a data communication network with no need for any physical transport of cards. Other features and advantages of

the invention appear from the description and claims below and from the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described in more detail with reference to specific embodiments thereof shown on the accompanying drawings.

Fig 1 is a schematic functional block diagram showing a prior art system for a digital transaction,

Fig 2 is a diagram showing an authorizing scheme that can be used in the system in Fig. 1,

Fig. 3 is a schematic functional block diagram showing a digital transaction system in accordance with the invention,

Fig. 4 is a schematic block diagram showing communication path in a device in accordance with the invention,

Fig. 5 is a diagram showing an authorizing scheme that can be used in the system in Fig. 3,

Fig. 6 is a schematic block diagram showing one embodiment of a device in accordance with the invention,

Fig. 7 is a schematic block diagram showing one embodiment of a smartcard that can be used with the device in Fig. 5,

Fig. 8 is a schematic perspective view of a first embodiment of a device in accordance with the invention and

Fig. 9 is a schematic perspective view of a second embodiment of a device in accordance with the invention.

## DETAILED DESCRIPTION

Fig. 1 shows a basic prior art system for digital transactions. A stationary terminal 10 is connected to a remote server 11 through a network 12. To provide an authorization of a user of the stationary terminal a smartcard 13 is inserted into the stationary terminal. The user enters personal identification data into the smartcard through the stationary terminal by using a user

interaction means 16. The user interaction means can be a keyboard or a device for the input of a biometric sample, such as a biometric sensor. The identification data unlocks the smartcard and enables authorization of the user and a secure communication between the stationary terminal and the remote terminal. However, the stationary terminal can be tampered with and the identification data can be obtained.

Fig. 2 shows a typical scheme where a user at a stationary terminal wants to be authorized by a remote network server. The scheme can be used in the prior art system shown in Fig. 1 and also in a system according to the present invention. The authentication process of the user (1) is performed first by entering personal identification data into the IC card. Then the stationary terminal requests to establish contact (2) with the remote server. The request is picked up and accepted (3) by the remote server. When contact has been established, the remote server sends a random number, called the challenge (4). The stationary terminal receives this number, encrypts it (6) together with an identification of the user and returns the result, called the response (6). At the remote server this message is decrypted, and the result compared with the challenge (7). If they are identical, it means that the IC card is authentic, since it uses the right key. The purpose of the random number is to ensure that the user is actually present and that the response is not just a replay of a message that has been recorded during some previous transaction. The steps 1-7 are essential in most communication schemes.

Every time a new number is sent as challenge. If the same encryption key is used, the encrypted messages will be different. Even if somebody is picking up the communication he cannot give the correct response to the next challenge trying to imitate the legitimate user.

Following this authentication of the user at the remote terminal there could for instance be a commercial transaction such as a credit card payment. The figure shows an example where the same cryptographic scheme is used as for the authentication.

Fig. 2 also shows further steps that are taken when a purchase is made. The remote server sends the amount to be paid (8) for the purchase. The amount is received by the stationary terminal (9) and confirmed by send-

ing the amount encrypted (10) as described above. The amount is received and decrypted by the remote server (11) and further checked locally (12). A confirmation finally is sent (13) by the remote server and received (14) by the stationary terminal. The steps 8-14 can be replaced by similar or corresponding steps for other types of transactions.

## PREFERRED EMBODIMENT

In a preferred embodiment as shown in Fig. 3 the electronics of a mobile terminal 14 is designed around a microcontroller 15 to which the smartcard 13 and all other main parts are connected. As a main feature of the invention the user interaction means 16 is included in the mobile terminal 14. All communication between the smartcard 13 and the user is carried out through the mobile terminal 14 (see Fig. 4 also). Thus, the user is authenticated by the smartcard through a device that can be protected against unauthorized operations. The smartcard is then authenticated by the stationary terminal 10 in a protected environment. The stationary terminal 10 can be authenticated by the remote server 11 through the network 12 in a conventional manner.

The protecting property of the mobile terminal 14 is apparent from Fig. 4. No transactions with the smartcard 13 can occur other than through the mobile terminal. This applies to the user 17 and to external devices such as the stationary terminal 10. All further transactions with the remote server and all transactions through an external network involving the smartcard will also be handled through the mobile terminal 14.

Fig. 5 shows a scheme where a user at a stationary terminal wants to be authorized by a remote network server when using a mobile terminal as shown in Fig. 3. The process is started when the user requests the mobile terminal to establish contact (1) with the remote server. The request is picked up and accepted (2) by the remote server. When contact has been established, the remote server sends a random number, called the challenge (3) back to the mobile terminal. The mobile terminal receives the random number (4). Before or during this session the user should be authenticated by the IC card. This could for instance be done as indicated by step (5). After au-

thentication the received random number is encrypted and returned (6) to the remote server. Finally, the encrypted number is decrypted and compared by the remote server (7). Further steps may then follow depending on the actual application.

In Fig. 6 the main units of a mobile terminal 14 are shown. The smartcard is mounted in a smartcard holder 18. In a preferred embodiment the smartcard holder is formed to allow a simple exchange of the smartcard. All main units of the mobile terminal 14 are controlled by the micro controller 15. The micro controller can be a conventional microprocessor or an application specific circuit. A program memory 19 holds the control program used by the micro controller and may be formed as a ROM. The software in the program memory controls all functions of the terminal. Data altering during execution is stored in a temporary scratchpad memory 20, such as a RAM.

The mobile terminal is also provided with means for user interaction. Data is presented to the user by an output unit 21, such as a LCD. Other types of displays and sound output means can also be used. An input unit 22, such as a keyboard or a device for input of biometric data, is also provided in the terminal.

A unit 23 for wireless communication with a stationary terminal is included and may include an IR or radio unit. There is also included means for communication with a stationary terminal via a physical connector 24. A flash disk 25 or similar device is provided for storing electronic documents produced during transactions and other larger data sets.

For communication the terminal must be capable of using protocols suitable for the different channels that are available, such as radio and IR. Even in the case a physical, electrical connection is used for communication a protocol must be used.

The smartcard contains a secure microprocessor with the following main parts as shown in Fig. 7. An interface 26 is provided for controlling the communication between the card and the terminal. The interface is connected to a processor 27 capable of performing all the necessary functions of the card, including protected access to memory and encryption/decryption of data. A ROM or flash memory 28 is used for storing programs, and a RAM 29

is used for storing temporary data. A permanent ID section of the card and optionally virtual cards is stored in an EEPROM 30.

The electronic parts of the mobile terminal as shown in Fig. 8 are contained in a cover 31 designed to be conveniently carried in a pocket, attached to a belt or similar arrangement. Power is provided by an internal battery (not shown). This and the smartcard can be replaced by the user. The smartcard has the size of a Plug-in SIM card (ETSI Standard GSM 11.11, Annex A). The output unit comprises a LCD 32, and the input unit comprises a keyboard 33, preferably including digit keys and a Yes and a No button. In the embodiment shown in Fig. 8 the input unit also comprises a biometric sensor 36 that identifies the fingerprint of the user. The wireless communication unit includes an IR window 34. Further means related to the wireless communication unit, such as an antenna or a coil, are covered by the cover 31.

Since smartcard readers are often available at transaction terminals it could be convenient to use these also to connect mobile terminals. In an alternative embodiment of the mobile terminal as shown in Fig. 9 one part of the terminal could be shaped as half a smartcard and have a set of smartcard connector pads 35 placed according to standard. This part of the terminal could then be inserted into a smartcard reader to provide an electrical connection between the terminals for communication. The terminal includes a LCD 32, a keyboard 33 and an IR window in conformity with the embodiment shown in Fig. 8.

After authentication of the user different further steps may be taken. A simple next step would be that the stationary terminal or a remote server registers the user and then allow access to data or to a closed and security protected area. In another application a key stored in the smartcard is used for the encryption of data to be sent from the stationary terminal to the remote server. In a third application an electronic purchase is requested and confirmed by the user. The purchase can then be recorded and executed by the remote server.

# CLAIMS

1. Method for secure digital data transactions, including the steps of:
   a) storing personal identification data, card identification data and a transaction program in a protected IC card,
   b) receiving personal identification data in said IC card,
   c) comparing said received personal identification data with said stored personal identification data and
   d) executing said transaction program when said personal identification data correspond to said stored personal identification data to establish contact between said IC card and a stationary terminal,

   characterized by
   e) mounting said IC card in a mobile unit,
   f) transferring said personal identification data to said IC card through said mobile unit, and
   g) further executing said transaction program to perform secure digital data transactions between said IC card and a stationary terminal through said mobile unit.

2. Method as claimed in claim 1, further including the steps of storing an encryption key in said protected IC card, executing said transaction program to transfer digital data from the stationary terminal to a remote server and applying said encryption key for encrypting digital data to be transferred.

3. Method as claimed in claim 1, further including the steps of connecting the mobile unit to the stationary terminal with a conductive coupling.

4. Method as claimed in claim 3, further including the steps of connecting the mobile unit to the stationary terminal through IC card connector pads arranged on the mobile terminal.

5. Method as claimed in claim 3, further including the steps of transferring digital data between the mobile unit and the stationary terminal through a wireless connection.

6. Method as claimed in claim 1, further including the steps of storing in said IC card a plurality of application specific card identification data sets, each set defining a virtual IC card.

7. A device for secure digital transactions including an IC card (13) containing protected personal identification data, card identification data and a transaction program,
characterized by a mobile terminal (14) comprising:

a) receiving means (18) for receiving said IC card (13),
b) input means (22) for entering personal identification data,
c) communication means (23; 24) for performing secure digital data transactions between said IC card and a stationary terminal (10).

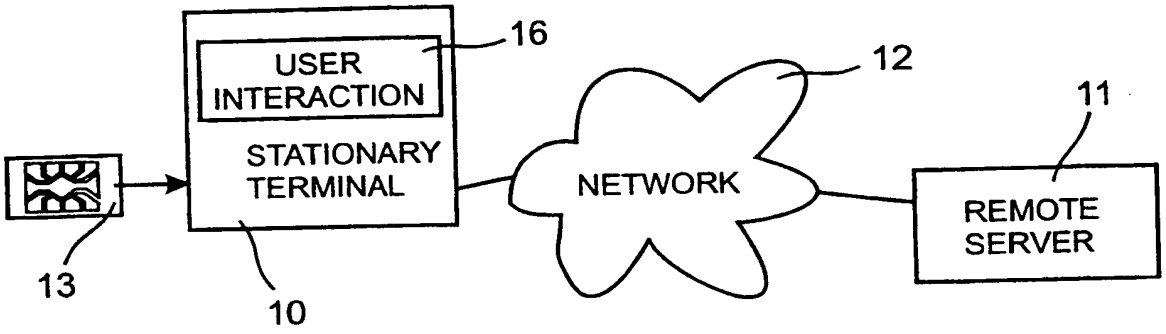
8. A device as claimed in claim 7, wherein said input means (22) comprises a biometric sensor (36).

9. A device as claimed in claim 7, wherein said communication means (23; 24) comprises IC card connector pads (35).

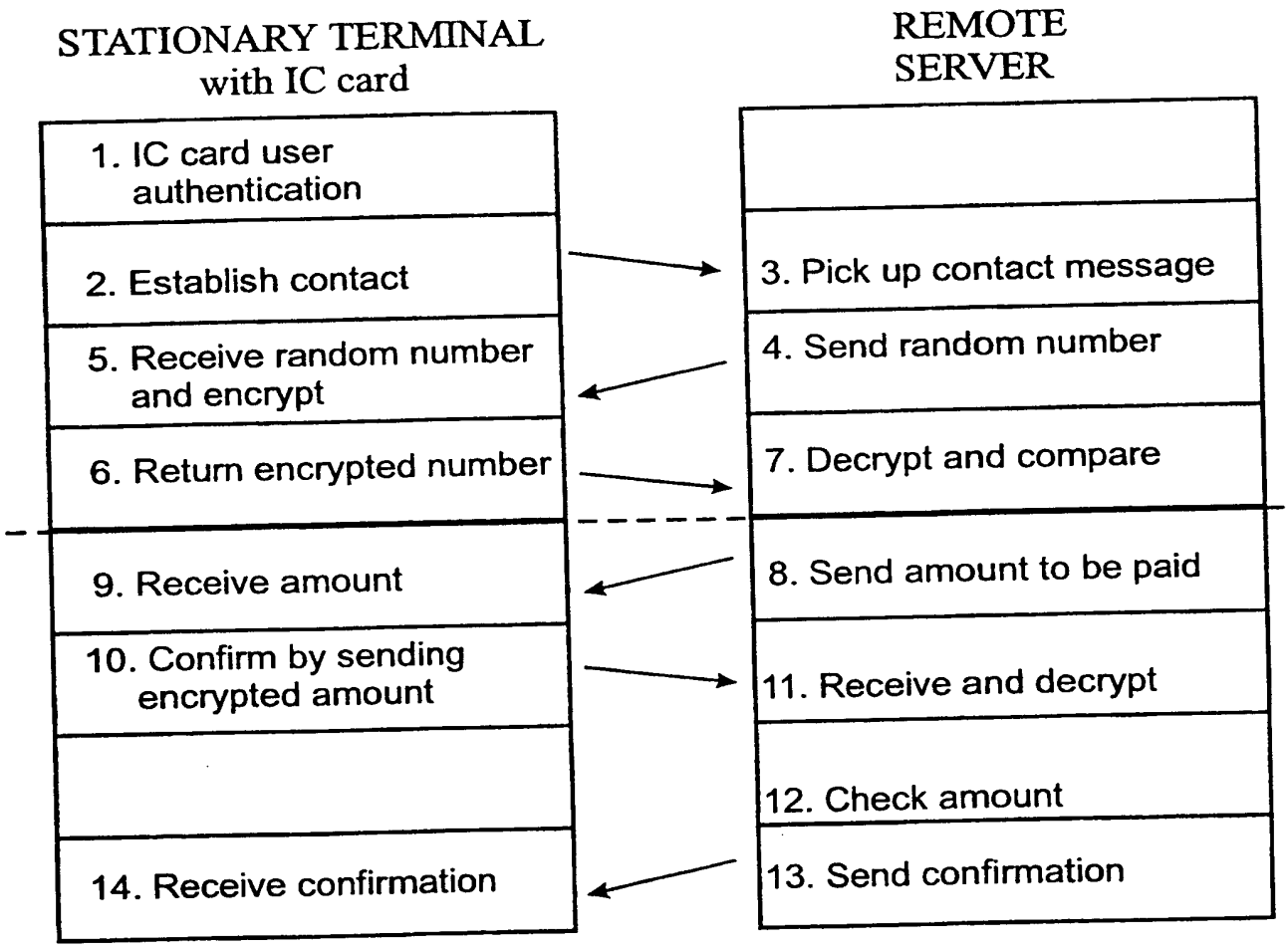
10. A device as claimed in claim 7, wherein said mobile terminal (14) is provided with display means (32).

11. A device as claimed in claim 7, wherein said receiving means (18) is operatively connected to a microcontroller (15) and said microcontroller (15) is operatively connected to said input means (22) for directing input data to an IC card received in said receiving means (18).

12. A device as claimed in claim 11, wherein said microcontroller (15) is operatively connected to storing means (25) for storing transaction history data.




PRIOR ART Fig. 1




PRIOR ART Fig. 2

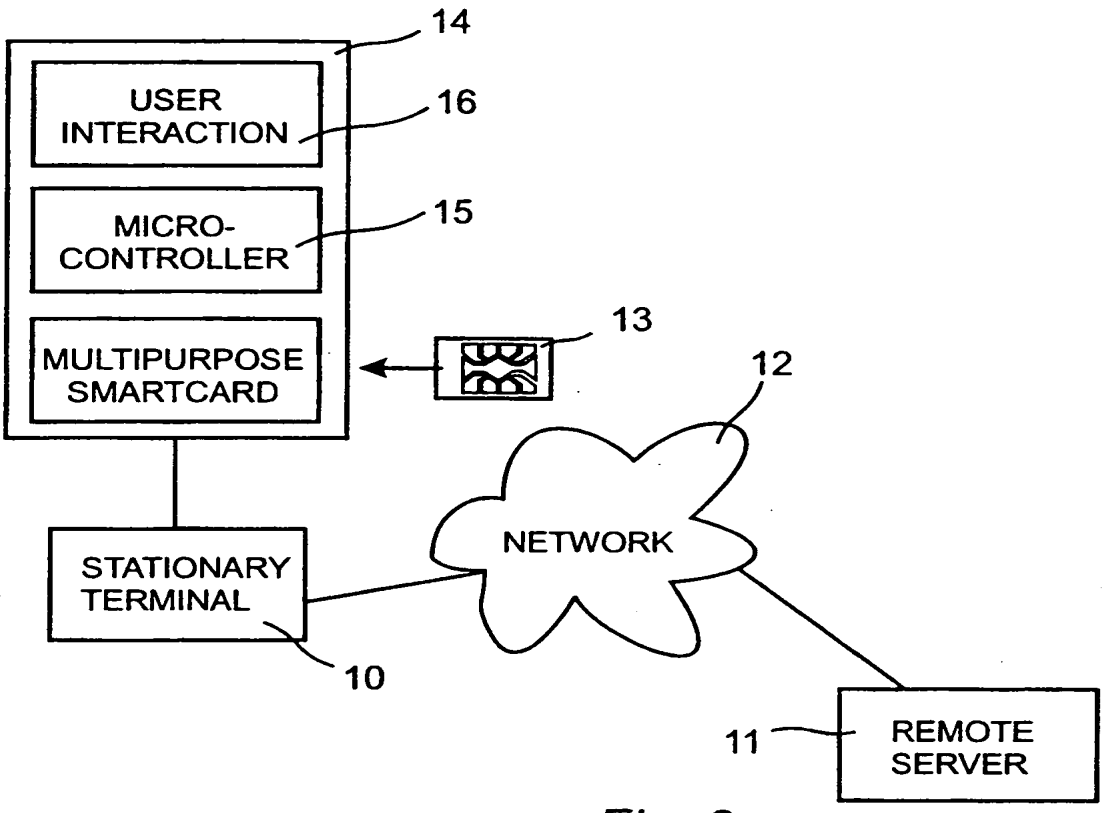

14
USER INTERACTION
16
MICRO-CONTROLLER
15
MULTIPURPOSE SMARTCARD
13
12
NETWORK
STATIONARY TERMINAL
10
11
REMOTE SERVER

Fig. 3

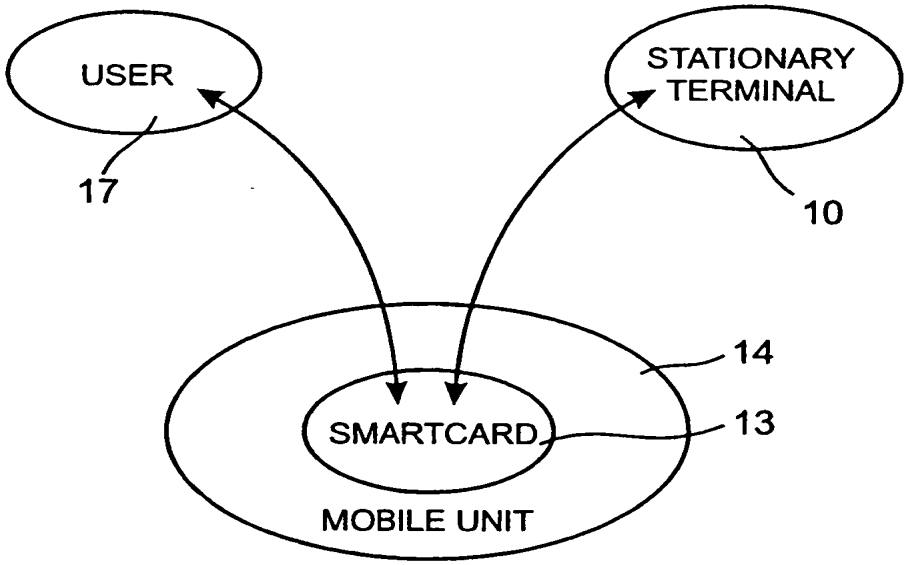

USER
17
STATIONARY TERMINAL
10
14
SMARTCARD
13
MOBILE UNIT

Fig. 4

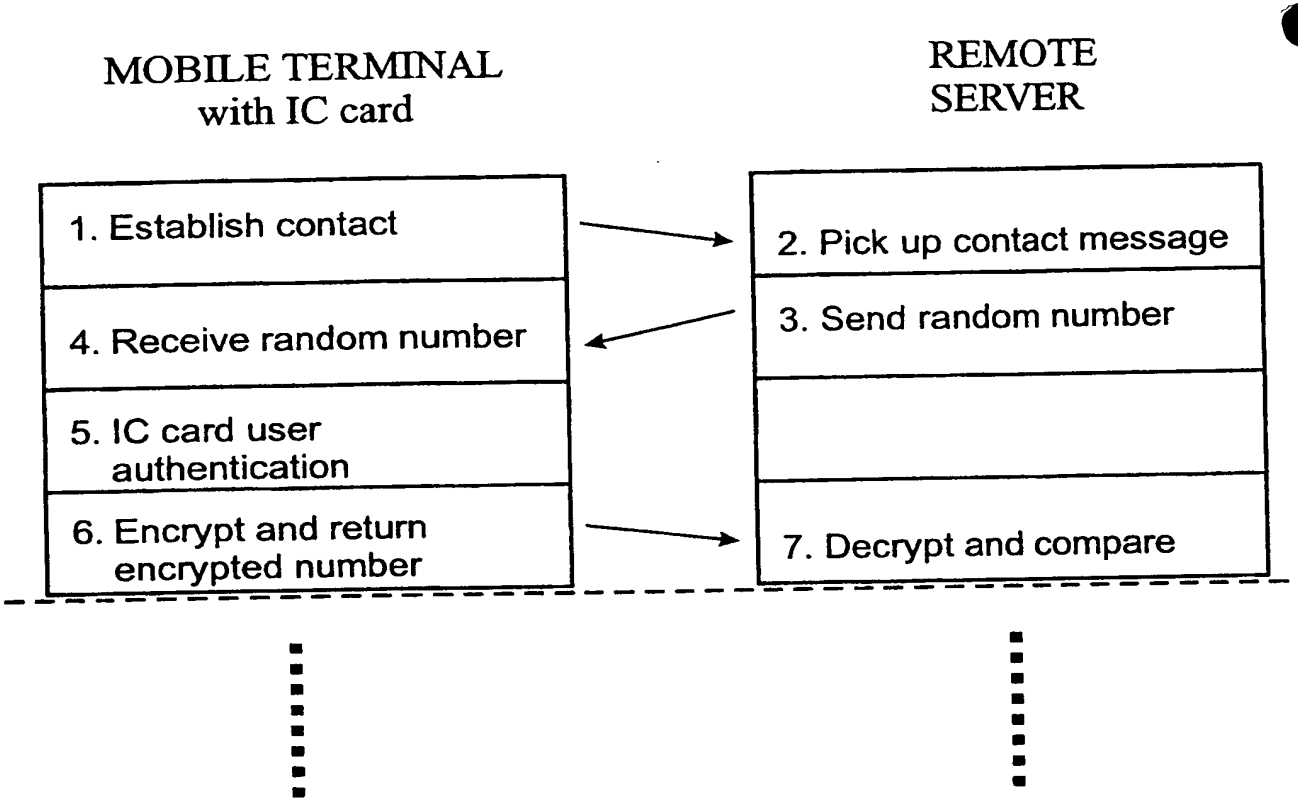

MOBILE TERMINAL
with IC card
REMOTE
SERVER
1. Establish contact
2. Pick up contact message
3. Send random number
4. Receive random number
5. IC card user
authentication
6. Encrypt and return
encrypted number
7. Decrypt and compare

*Fig. 5*

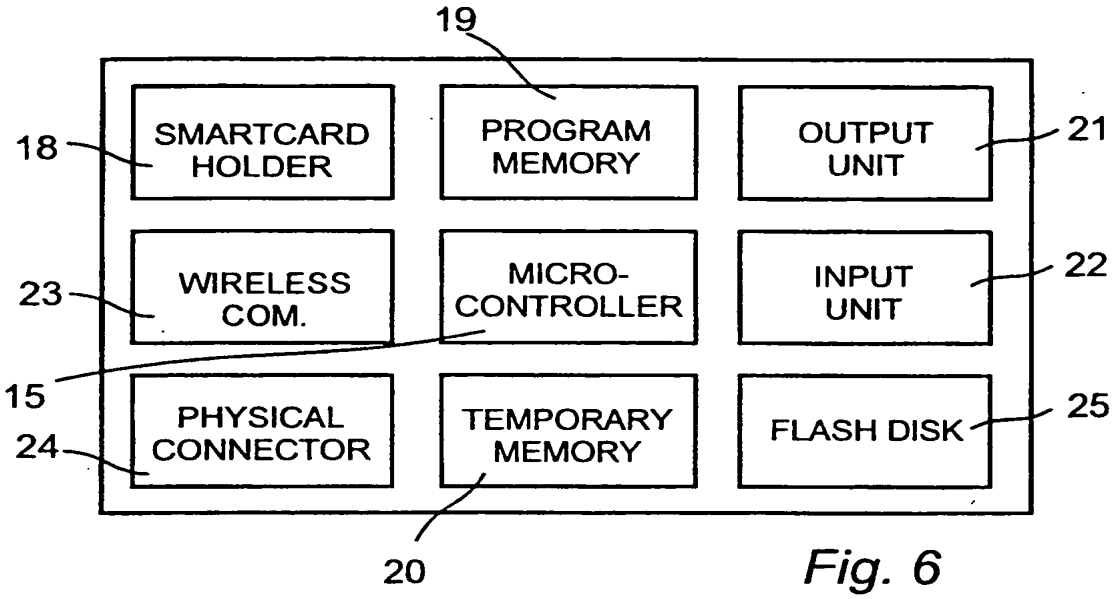

19
SMARTCARD HOLDER
PROGRAM MEMORY
OUTPUT UNIT
18
21
WIRELESS COM.
MICRO-CONTROLLER
INPUT UNIT
23
22
15
PHYSICAL CONNECTOR
TEMPORARY MEMORY
FLASH DISK
24
25
20

Fig. 6

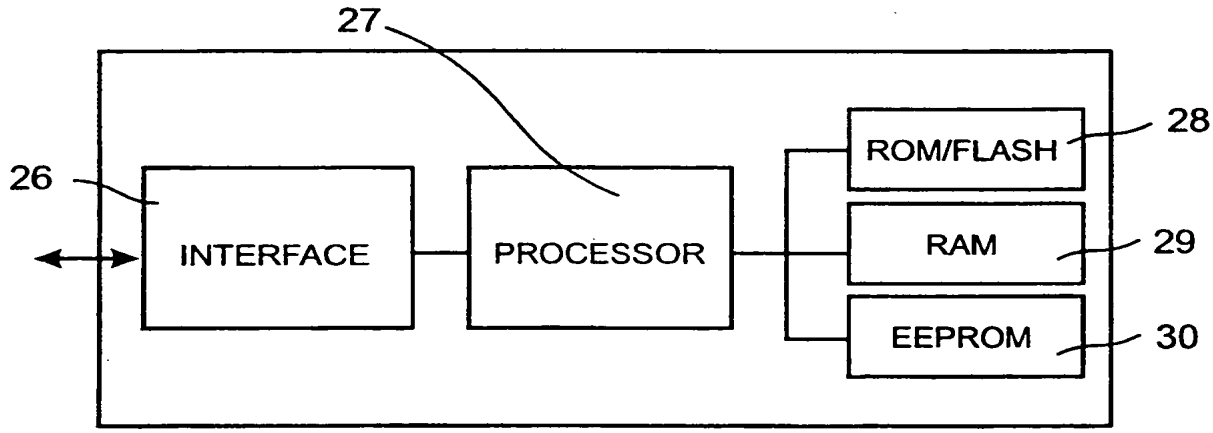

27
ROM/FLASH
28
26
INTERFACE
PROCESSOR
RAM
29
EEPROM
30

Fig. 7

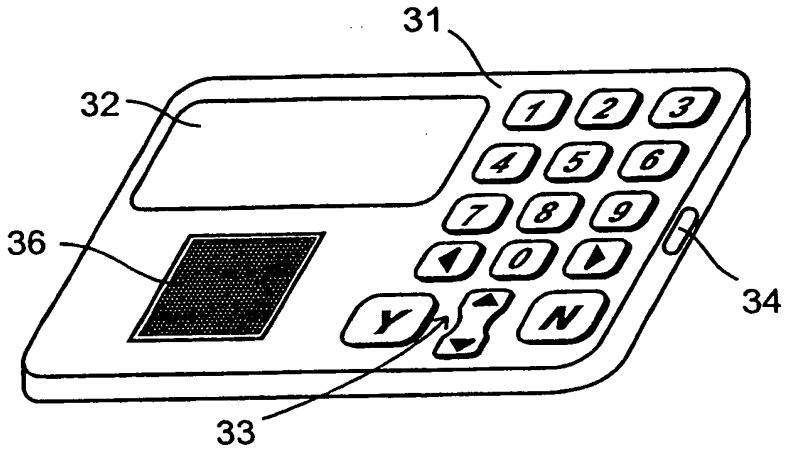



Fig. 8

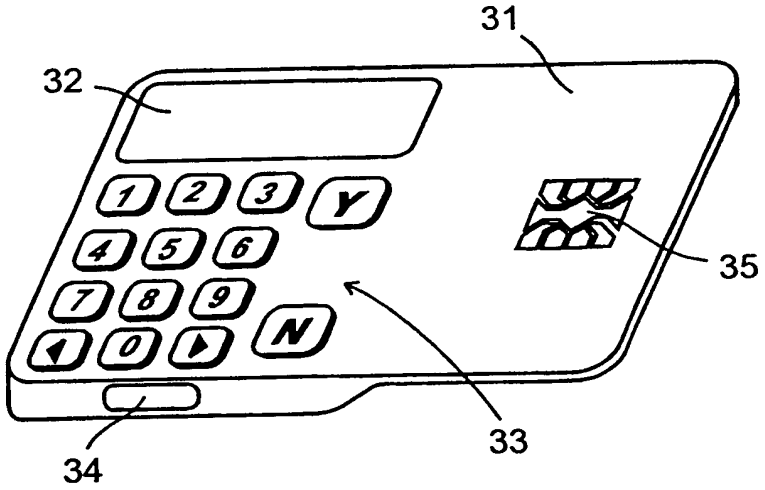



Fig. 9

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/00563

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/60, H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI-DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5796832 A (J.C.KAWAN), 18 August 1998 (18.08.98), column 4, line 4 - line 14; column 8, line 52 - line 54, figures 1,2c, claim 1, abstract | 1-5,7-12 |
| Y | -- | 6 |
| Y | US 5748737 A (R.N.DAGGAR), 5 May 1998 (05.05.98), abstract | 6 |
| | -- | |
| A | US 6016476 A (S.H.MAES ET AL.), 18 January 2000 (18.01.00), column 2, line 23 - column 4, line 11, abstract | 1-12 |
| | -- | |

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 21 May 2001 | 19 -06- 2001 |
| Name and mailing address of the ISA/<br>Swedish Patent Office<br>Box 5055, S-102 42 STOCKHOLM<br>Facsimile No. +46 8 666 02 86 | Authorized officer<br>Pär Heimdal/LR<br>Telephone No. +46 8 782 25 00 |

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/00563

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 0011624 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 2 March 2000 (02.03.00), page 3, line 16 - line 27, figures 1-2, claims 1,12, abstract<br>-- | 1-12 |
| P,A | US 6098055 A (M.WATANABE), 1 August 2000 (01.08.00), column 1, line 66 - column 2, line 19, claim 1, abstract<br>-- | 1-12 |
| P,A | US 6142369 A (U.JONSTROMER), 7 November 2000 (07.11.00)<br>--<br>-------- | 1-12 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

30/04/01

International application No.
PCT/SE 01/00563

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5796832 A | 18/08/98 | AU 1074597 A | 05/06/97 |
| | | BR 9611515 A | 02/03/99 |
| | | CN 1202287 A | 16/12/98 |
| | | EP 0872075 A | 21/10/98 |
| | | JP 2000500595 T | 18/01/00 |
| | | WO 9718653 A | 22/05/97 |
| US 5748737 A | 05/05/98 | NONE | |
| US 6016476 A | 18/01/00 | EP 1004099 A | 31/05/00 |
| | | IL 130068 D | 00/00/00 |
| | | PL 338353 A | 23/10/00 |
| | | WO 9908238 A | 18/02/99 |
| | | TW 385400 B | 00/00/00 |
| WO 0011624 A1 | 02/03/00 | AU 5767299 A | 14/03/00 |
| US 6098055 A | 01/08/00 | AU 721600 B | 06/07/00 |
| | | AU 1257197 A | 14/08/97 |
| | | CA 2196947 A | 08/08/97 |
| | | GB 2310069 A,B | 13/08/97 |
| | | GB 9702492 D | 00/00/00 |
| | | JP 9212565 A | 15/08/97 |
| US 6142369 A | 07/11/00 | AU 3943795 A | 06/06/96 |
| | | EP 0784715 A | 23/07/97 |
| | | EP 0958556 A | 24/11/99 |
| | | JP 10508904 T | 02/09/98 |
| | | NO 974626 A | 13/10/97 |
| | | SE 506506 C | 22/12/97 |
| | | SE 9501347 A | 12/10/96 |
| | | WO 9632700 A | 17/10/96 |